

# CYBER SECURITY

September 2008

Monthly Awareness Newsletter

## TOP 7 SECURITY MYTHS & MISTAKES

### Background

It seems like every week we learn about a new store, bank or government organization that is hacked into with millions of dollars lost, information stolen or identities compromised. These stories often follow with details on how to protect yourself and your organization. However, even with all this media attention there are still many misconceptions about cyber security. Below we list seven of the most common misconceptions and explain what you can do to protect yourself.

**1. I Am Not A Target:** This is the number one misconception as too many people mistakenly believe they are not targeted, that only large corporations or government organizations are attacked. What value could one person or computer have? Actually, it is the individuals that are the primary targets, criminals continuously attack people all over the world, including you. The reason that such attacks receive very little coverage in media is because individuals do not contribute to exciting stories, big organizations do. The first step in protecting yourself is understanding you are actually the primary target.

**2. I Am Safe, I Turn My Computer Off At Night:** Many people assume that if they turn off their computer when it is not in use they are less likely to be attacked. Unfortunately, this is no longer true. First, criminals are so aggressive that being online for just one hour a day exposes you to almost the same types of risks as if you were online twenty four hours a day. Second, most of today's attacks occur when you interact with the Internet, by Instant Messaging, surfing the World Wide Web or reading email. Turning off computer will not protect you, using your computers securely will.

**3. I Am Safe, My IP Address Changes:** Many people use computers, either at home or at work, that are on DHCP networks, meaning that every time they connect to the network they get a new IP address. IP (Internet Protocol) addresses are how systems on the Internet find specific computers. However, having the IP address change often does not protect the computer. Criminals simply target every single computer on the Internet every single day of the year. Changing your IP address has very little effect, using your computer safely will.



### Common Myths and Mistakes

*By understanding these common myths and mistakes and not falling for them, you will go a long way in protecting yourself and your organization.*

## HONEYTECH

This free security newsletter is published every month. Sign up for your free newsletter at

<http://www.honeytech.com>

HoneyTech will be teaching a three day security awareness course for management at Dubai this 16-18 November.

<http://www.meitsec.ae>

# How Do I Protect Myself?

After reading about these common myths you may think it is impossible to protect yourself. Fortunately, this is not the case. The key is not what security tools you install, the key is safe habits.

Securing yourself on the Internet is similar to driving your car. There is a great deal of technology installed in your car to protect you in case of accident, such as air bags and seat belts. But safe driving habits that prevent accidents is the best protection of all. The same logic applies to using computers and the Internet. Some key steps that will protect you include:

- Make sure your operating system and applications (such as your web browser) are always updated to the most current version.
- Open attachments only from people you know and only when you expect the attachments.
- Criminals use email and Instant Messaging to fool people, do not trust suspicious emails. They often pretend to be from trustworthy organizations, such as banks, or use lottery scams to ask for your information. No legitimate organization will use email to ask unsolicited for your private information.
- Install applications you absolutely need and then only from trusted sources.
- Do not share your passwords with anyone. Use different passwords for different websites or applications, ensure they are hard to guess and change them every ninety days.

## 4. I Am Safe, I Use Anti-Virus:

Several years ago anti-virus could protect you against most infected programs or software attacks but not anymore. Criminals have become far more organized and advanced, their viruses and trojans can often bypass even the most advanced anti-virus technologies. Some criminals even specialize in developing software aimed at bypassing anti-virus and sell their tools and services to other criminals. Anti-virus is still an important tool and you need to have it installed but it does not protect you all the time. The best way to ensure that your computer does not become infected is to install only the software you know and trust.

## 5. I Am Safe, I Am Behind A

**Firewall:** Many computers at home or work sit behind a firewall. A firewall protects your computer by allowing you to connect to the Internet (such as visiting websites or downloading email) but prevents other computers from initiating a connection to you. While firewalls protect against older attacks, such as worms, they do not protect you against the latest attacks, such as infected emails or malicious websites. Safe and secure Internet habits are the best way to protect against the latest threats.

## 6. Security Is Only A Problem In America or Europe, No One Targets My Country:

Many people mistakenly believe that criminals only attack western countries, that there are no attacks in their own country. Nothing could be farther from the truth. Criminals simply target every computer and culture in the world. It is very cheap and highly profitable for them to do so. It does not matter if you speak Arabic, live in Asia or travel in South America, you are still a target.

## 7. I Can Trust Public Computers:

The only computers you want to trust are those you control. For example, do not trust public computers in libraries, kiosks, conferences or Internet cafes. You can use these computers for common tasks such as reading websites, but do not use them for private activities such as online banking or reading company email. The organizations providing these computers are most likely trustworthy, but what about the person who used the computer before you? Perhaps that person before you was a criminal and infected the computer on purpose. Or perhaps that person was not security aware and unknowingly downloaded infected software. Never trust public computers for your private activities.

### More Information

Here are some additional sites and resources

- Protecting Yourself: <http://onguardonline.gov>  
Protecting Your Windows Computer: <http://www.microsoft.com/protect/default.aspx>  
Anti-virus Rankings: [http://mtc.sri.com/live\\_data/av\\_rankings/](http://mtc.sri.com/live_data/av_rankings/)  
F-Secure Trends For 2008: <http://www.fsecure.com/2008/1/index.html>  
Dancho Danchev Security Blog: <http://ddanchev.blogspot.com>